



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/522,919

01/31/2005

Paul W Hodgson

36-1885

4217

23117

7590

02/06/2008

NIXON & VANDERHYE, PC

901 NORTH GLEBE ROAD, 11TH FLOOR

ARLINGTON, VA 22203

EXAMINER

TAHA, SHAQ

ART UNIT

PAPER NUMBER

2146

MAIL DATE

DELIVERY MODE

02/06/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.		Applicant(s)	
	11/097,331		ESTABLE, LUIS PABLO	
	Examiner		Art Unit	
	Shaq Taha		2146	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE ____ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☐ Claim(s) ____ is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☐ Claim(s) ____ is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. ____. |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date ____. | 6) <input type="checkbox"/> Other: ____. |

DETAILED ACTION

This is a final action for application number 10/522,919 based on after non-final filed on 10/25/2007. The original application was filed on 01/31/2005. Claims 1 – 36 are currently pending and have been considered below. Claims 1, 12, 20, 23, 31, 32, and 36 are independent claims.

Applicant's Response

In the applicant's response dated 10/25/2007; the applicant argued against all the rejections set forth on the non-final rejection on 07/25/2007.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

- Claims, 1 – 4, 11 – 15, 19, 22, 28, 30 – 32, and 34 – 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hile et al. (US 5,319,776), and further in view of Sorkin et al. (US 2002/0162017).

Regarding claim 1, Hile teaches a server configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, each terminal being accessed by one or more users, **[Data is tested in transit between a source medium and a destination medium, such as between two computer communicating over a telecommunications link or network, (See Abstract)]**;

the server comprising: receiving means arranged to generate or receive log data relating to one or more traffic characteristics associated with electronic messages, **[Testing log data when it is in transit between a source and a destination and depending on the traffic characteristic the incoming data could be prevented from remaining on the destination, (Abstract)]**;

analyzing means arranged to analyze the log data in accordance with a predetermined criterion, so as to identify those electronic messages that satisfy the criterion, **[The present invention intervenes at this point by subjecting the buffered data to a character by character virus signature string search analysis depicted, (Column 4, lines 11 – 13)]**;

identifying means arranged to identify the destination of the identified electronic messages, **[The method comprises the steps of causing a transmission of digital data resident on a source storage medium to be transmitted to a computer system having a destination storage medium, (Column2, lines 21 – 25)]**;

processing means arranged to send a message to each of the identified destinations, **[The invention will be described in conjunction with a communications system**

which may be used to send and receive data via modems over a telecommunications link, (Column 3, lines 7 – 10));

requesting suspension of delivery of the identified electronic messages, **[When a virus is detected the incoming data is prevented from remaining on the destination storage medium, (See Abstract)];**

Hile differs from the claimed invention is that log data is not taught in Hile.

Sorkin et al. teaches a system and method for providing security for a computer network;

Sorkin further teaches various actions and events may be recorded in a log file, and the log file is analyzed using regular expressions, **(Abstract)**.

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Hile by including log data as taught by Sorkin.

One of ordinary skill in the art would have been motivated to make this modification in order provide the advantage of generating log data.

Regarding claim 2, Hile teaches a server including first means arranged to receive a signal identifying whether or not an identified electronic message is related to an electronic message virus, **[When a virus is detected the incoming data is prevented from remaining on the destination storage medium, (See Abstract);** second means arranged to receive data indicative of the success or otherwise of the request, and, in the event that the received signal identifies an electronic message to be a virus and the request is successful, to trigger deletion of the said electronic message, **[When a virus**

is detected the incoming data is prevented from remaining on the destination storage medium, (See Abstract)].

Regarding claim 3, Hile teaches a server wherein, in the event that a received signal identifies an electronic message to be a virus and the request is unsuccessful, **[When a virus is detected the incoming data is prevented from remaining on the destination storage medium, (See Abstract);**

the second means is arranged to trigger operation of identifying means and processing means running on a server corresponding to the destination of the identified electronic message, **[When a virus is detected the incoming data is prevented from remaining on the destination storage medium, (See Abstract).**

Regarding claim 4, Hile teaches a server wherein, in the event that a received signal identifies an electronic message not to be a virus and the request is successful, the second means is arranged to permit delivery of the identified electronic message, **[To combat the problem, others have employed virus scanning programs which read the files stored on a storage medium, looking for known virus signatures, (Column 1, lines 32 – 35)].**

Regarding claim 11, Hile teaches an apparatus wherein the criterion includes at least one of electronic message, size of electronic message and number of electronic messages emanating from a user, **[It is assumed in this example that the user**

wishes to copy a file from the removable diskette medium to the hard disk medium, (Column 4, lines 33 – 35)].

Regarding claim 12, Hile teaches a method of controlling propagation of electronic messages through a network, **[Data is tested in transit between a source medium and a destination medium, such as between two computer communicating over a telecommunications link or network, (See Abstract)];**

the network comprising a plurality of servers configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, **[The invention will be described in conjunction with a communications system which may be used to send and receive data via modems over a telecommunications link, (Column 3, lines 7 – 10)];**

each terminal being accessed by one or more users, **[In a telecommunications system, often the user of the second computer system 14 will have no direct control over the integrity of files stored on the source medium, (Column 3, lines 45 – 48)];**

the method comprising receiving or generating traffic log data relating to one or more traffic characteristics associated with electronic messages sent from, or received at, a said server, , **[The invention will be described in conjunction with a communications system which may be used to send and receive data via modems over a telecommunications link, (Column 3, lines 7 – 10)];**

analyzing the received data in accordance with a specified criterion, so as to identify those electronic messages that satisfy the criterion, **[To combat the problem, others have employed virus scanning programs which read the files stored on a storage medium, looking for known virus signatures, (Column 1, lines 32 – 35)].**

identifying the destination of the identified electronic messages, **[Fig.1, Step 40];**
and sending a message to each of the identified destinations, requesting suspension of delivery of the identified electronic messages, **[When a virus is detected the incoming data is prevented from remaining on the destination storage medium, (See Abstract).**

Regarding claim 13, Hile teaches a method including receiving a signal identifying whether or not an identified electronic message is related to an electronic message virus, **[When a virus is detected the incoming data is prevented from remaining on the destination storage medium, (See Abstract);**
receiving data indicative of the success or otherwise of the request, and, in the event that the received signal identifies an electronic message to be a virus and the request is successful, triggering deletion of the said electronic message, **[If a virus was detected during the transfer, the routine at step 78 can be made to purge the data in the file by overwriting it with 1's or 0's and the file is then deleted from storage, (Column 7, (lines 24 – 31))];**

Regarding claim 14, Hile teaches a method wherein, in the event that a received signal identifies an electronic message to be a virus and the request is unsuccessful, **[When a**

virus is detected the incoming data is prevented from remaining on the destination storage medium, (See Abstract);

the method includes triggering the identifying and sending steps to be carried out in respect of a server corresponding to the destination of the identified electronic message, **[The invention will be described in conjunction with a communications system which may be used to send and receive data via modems over a telecommunications link, (Column 3, lines 7 – 10)];**

Regarding claim 15, Hile teaches a method wherein, in the event that a received signal identifies an electronic message not to be a virus and the request is successful, the method includes triggering delivery of the identified electronic message, **[Since the conventional virus scanning program tests files which are already stored on the computer system's storage media, such programs simply alert the user that the computer has a virus, (Column 1, lines 45 – 48)].**

Regarding claim 19, Hile teaches a method wherein the criterion includes at least one, of (a) type of electronic message, (b) size of electronic message and (c) number of electronic messages emanating from a user, **[It is assumed in this example that the user wishes to copy a file from the removable diskette medium to the hard disk medium, (Column 4, lines 33 – 35)].**

Regarding claim 22, Hile teaches tangibly storage media containing a computer program, or a suite of computer programs, comprising a set of instructions to cause a

computer, or a suite of computers, to perform the method, **[Although described using examples written in the C programming language, this should not be viewed as a limitation, since numerous computer languages could be selected for implementing the invention, (Column 10, lines 19 – 24)].**

Regarding claim 28, Hile teaches a terminal wherein the terminal is configured to detect whether a criterion relating to the specified electronic message is met, and to request a confirmation input from a user at the user interface in response to the criterion being met, **[As each successive character enters, it is tested and if a character match is found, the machine state will toggle forward in the direction of the arrows, (Column 5, lines 2 – 6)].**

Regarding claim 30, Hile teaches a tangibly storage medium having a computer program stored thereon, the computer program being executable on a terminal so as to cause the terminal to operate, **[Although described using examples written in the C programming language, this should not be viewed as a limitation, since numerous computer languages could be selected for implementing the invention, (Column 10, lines 19 – 24)].**

Regarding claim 31 & 32, Hile teaches a tangibly storage medium having a computer program thereon for sending and receiving electronic messages, the program being executable on a terminal having a user interface, **[A communications system which**

may be used to send and receive data via modems over a telecommunications link, (Column 3, line 8)];

the computer program being configured to perform the following steps when executed:

(a) invite a user to input at the user interface send instructions for sending one or more electronic messages, **[A communications system which may be used to send and receive data via modems over a telecommunications link, wherein in the communication system a user is sending the data, (Column 3, line 8)];**

(b) determine if traffic log data meets a predetermined criterion relating to the electronic messages is met, **[Testing log data when it is in transit between a source and a destination and depending on the traffic characteristic the incoming data could be prevented from remaining on the destination, (Abstract)];**

(c) if the criterion is met, invite the user to input at the user interface a confirmation input to confirm the send instructions, **[The virus detection function informs the user that a virus has been detected and gives the user the option to cancel the transfer by setting the Virus Detected Flag, (Column 7, line 3)];**

(d) upon receipt of the confirmation input, transmit the electronic messages from the terminal, **[The virus detection function informs the user that a virus has been detected and gives the user the option to cancel the transfer by setting the Virus Detected Flag, (Column 7, line 3)];**

and (e) transmit authentication data associable with the transmitted electronic message (s), **[Although described using examples written in the C programming language,**

this should not be viewed as a limitation, since numerous computer languages could be selected for implementing the invention, (Column 10, lines 19 – 24)].

Regarding claim 34, Hile teaches a carrier wherein the computer program thereon is configured, when executed, to request a user to input password data as part of the confirmation instructions, and to only permit the terminal to send authentication data once the password data has been input by the user, **[Although described using examples written in the C programming language, this should not be viewed as a limitation, since numerous computer languages could be selected for implementing the invention, (Column 10, lines 19 – 24)].**

Regarding claim 35, Hile teaches a server wherein the criterion is met if log data relating to a target electronic message indicates that a threshold number of electronic messages and/or a threshold data volume originate from a common terminal or user, in a time interval during which the target electronic message was sent, **[By use of an assignable Machine Handle, the invention is able to support separate simultaneous data transfers which may overlap in time, (Column 6, lines 47 – 50)].**

Regarding claim 36, Hile teaches a server configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, **[Data is tested in transit between a source medium and**

a destination medium, such as between two computer communicating over a telecommunications link or network, (See Abstract)];

each terminal being accessed by one or more users, **[In a telecommunications system, often the user of the second computer system 14 will have no direct control over the integrity of files stored on the source medium, (Column 3, lines 45 – 48)];**

the server comprising: receiving means arranged to generate or receive log data relating to such electronic messages, **[The invention will be described in conjunction with a communications system which may be used to send and receive data via modems over a telecommunications link, (Column 3, lines 7 – 10)];**

analyzing means arranged to analyze the traffic log data in accordance with a specified criterion, so as to identify those electronic messages that satisfy the criterion, **[To combat the problem, others have employed virus scanning programs which read the files stored on a storage medium, looking for known virus signatures, (Column 1, lines 32 – 35)];**

identifying means arranged to identify the destination of the identified electronic messages, **[Fig.1, step 40];**

processing means arranged to send a message to each of the identified destinations, requesting suspension of delivery of the identified electronic messages, **[The invention will be described in conjunction with a communications system which may be**

used to send and receive data via modems over a telecommunications link,
(Column 3, lines 7 – 10)].

- Claims, 5 – 7, 8 – 10, 16 – 18, 20, 21, 25 - 29, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hile et al. (US 5,319,776) as applied to claims 1 above, and further in view of Kim et al. (US 6,701,440).

Regarding claim 5, Hile teaches a server including first storage for storing details relating to such electronic messages, **[Fig.1, step 40]**;

further storage for storing a mapping between users and the organizational units to which the users belong, **[Fig.1, step 40]**;

wherein the server is arranged, in use, such that in response to a request for data relating to a user, the first storage is arranged to output data identifying electronic messages emanating from that user, **[Fig.1, step 40]**;

the further storage is arranged to output data identifying which of the organizational units that user belongs to; and, for those electronic messages that are identified to satisfy the criterion, **[Fig.1, step 40]**;

Hile further teaches an apparatus for delivering electronic messages, comprising a plurality of servers; wherein at least one of the servers comprises: receiving means arranged to receive a request to suspend delivery of an identified electronic message, **[The invention will be described in conjunction with a communications system**

which may be used to send and receive data via modems over a telecommunications link, (Column 3, lines 7 – 10)].

Regarding claim 6, Hile teaches a server wherein, for those electronic messages that are identified to satisfy the criterion, the display means is arranged to display a list of users on an associated image, and for each user on the list, to display details of the volume and/or type of identified electronic messages emanating therefrom, **[Since the conventional virus scanning program tests files which are already stored on the computer system's storage media, such programs simply alert the user that the computer has a virus, (Column 1, lines 48 – 51)].**

Regarding claim 7, Hile teaches a server wherein the display means is arranged to insert a link between the identified organizational unit and the organizational unit corresponding to the identified destination, **[Data is tested in transit between a source medium and a destination medium, such as between two computer communicating over a telecommunications link or network, (See Abstract)].**

Regarding claim 18, Hile teaches a method including inserting a link between the identified organizational unit and the organizational unit corresponding to the identified destination, **[Data is tested in transit between a source medium and a destination medium, such as between two computer communicating over a telecommunications link or network, (See Abstract)].**

Regarding claim 20, Hile teaches a method of identifying electronic message activity within an organization, the organization having a plurality of users associated therewith, each of which is connected with an organizational unit, **[In a telecommunications system, often the user of the second computer system 14 will have no direct control over the integrity of files stored on the source medium, (Column 3, lines 45 – 48)]**;

the method comprising: receiving traffic log data defining at least one message traffic characteristic emanating from a user relating to electronic messages sent by a user, **[The invention will be described in conjunction with a communications system which may be used to send and receive data via modems over a telecommunications link, (Column 3, lines 7 – 10)]**;

analyzing the received traffic log data in accordance with a specified criterion, so as to identify those electronic messages that satisfy the criterion, **[To combat the problem, others have employed virus scanning programs which read the files stored on a storage medium, looking for known virus signatures, (Column 1, lines 32 – 35)]**.

Regarding claim 21, Hile teaches a method wherein the criterion includes any one, or some, of type of electronic message, size of electronic message and number of electronic messages emanating from a user, **[It is assumed in this example that the user wishes to copy a file from the removable diskette medium to the hard disk medium, (Column 4, lines 33 – 35)]**.

Hile et al. differs from the claimed invention is that the method includes displaying a list of users on an associated image, and for each user on the list, displaying details of the volume and/or type of identified electronic messages emanating therefrom is not taught in Hile et al.

Kim teaches a system and method for a remote or network-based application service offering virus scanning, sniffing, or detecting of e-mail viruses prior to the e-mail messages arriving at the destination system or server are disclosed. The method protects a computer system that is configured to receive an e-mail message addressed to a destination e-mail address from viruses in an incoming e-mail message, (**See Abstract**), and further teaches that FIG. 5 shows a computer system 500 that includes a display or monitor 502, screen 504, cabinet 506, keyboard 508, and mouse 510, (**Column 11, lines 48 - 52**). Kim provides the advantage of checking whether or not the identified electronic message has been delivered.

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Hile by including displaying a list of users on an associated image, and for each user on the list, displaying details of the volume and/or type of identified electronic messages emanating therefrom as taught by Kim.

One of ordinary skill in the art would have been motivated to make this modification in order provide the advantage of FIG. 5 shows a computer system 500 that includes a display or monitor 502, screen 504, cabinet 506, keyboard 508, and mouse 510.

- **Claims 8 – 10** are rejected under 35 U.S.C. 103(a) as being unpatentable over Hile et al. (US 5,319,776) as applied to claims 1 above, and further in view of Kim et al. (US 6,701,440).

Regarding claim 8, Hile teaches the method according to claim 1, as described above.

Hile further teaches an apparatus for delivering electronic messages, comprising a plurality of servers; wherein at least one of the servers comprises: receiving means arranged to receive a request to suspend delivery of an identified electronic message, **[The invention will be described in conjunction with a communications system which may be used to send and receive data via modems over a telecommunications link, (Column 3, lines 7 – 10)]**.

Regarding claim 9, Hile teaches an apparatus wherein the at least one server includes deleting means for deleting an electronic message, **[If a virus was detected during the transfer, the routine can be made to purge the data in the file by overwriting it with 1's or 0's and the file is then deleted from storage, (Column 7, (lines 24 – 31))**; and, in response to receipt of a signal identifying that an identified electronic message is related to an electronic message virus, **[When a virus is detected the incoming data is prevented from remaining on the destination storage medium, (See Abstract)]**. the deleting means is arranged to check whether retrieval of the identified electronic message has been blocked, and if it has, to delete it, **[If a virus was detected during**

the transfer, the routine can be made to purge the data in the file by overwriting it with 1's or 0's and the file is then deleted from storage, (Column 7, (lines 24 – 31));

Regarding claim 10, Hile teaches an apparatus wherein, in the event that the identified electronic message is related to an electronic message virus, and the identified electronic message has not been blocked, **[If a virus was detected during the transfer, the routine can be made to purge the data in the file by overwriting it with 1's or 0's and the file is then deleted from storage, (Column 7, (lines 24 – 31));** The server is arranged to invoke its identifying means and processing means in respect of electronic messages sent by the identified destinations, **[If a virus was detected during the transfer, the routine at step 78 can be made to purge the data in the file by overwriting it with 1's or 0's and the file is then deleted from storage, (Column 7, (lines 24 – 31));**

Hile et al. differs from the claimed invention is that check whether or not the identified electronic message has been delivered is not taught in Hile et al.

Kim teaches a system and method for a remote or network-based application service offering virus scanning, sniffing, or detecting of e-mail viruses prior to the e-mail messages arriving at the destination system or server are disclosed. The method protects a computer system that is configured to receive an e-mail message addressed to a destination e-mail address from viruses in an incoming e-mail message, **(See Abstract)**, and further teaches that A VPN (virtual private network) may additionally or alternatively be utilized in order to ensure the security of the e-mail messages being

delivered, (**Column 8, lines 7 - 10**). Kim provides the advantage of checking whether or not the identified electronic message has been delivered.

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Hile by including checking whether or not the identified electronic message has been delivered as taught by Kim.

One of ordinary skill in the art would have been motivated to make this modification in order provide the advantage of providing the advantage of checking whether or not the identified electronic message has been delivered.

- **Claims** 25 - 29, and 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hile et al. (US 5,319,776) as applied to claims 1 above, and further in view of Kim et al. (US 6,701,440).

Regarding Claims 25 - 29, and 33, Hile teaches the method according to claim 1, as described above. Hile further teaches Data is tested in transit between a source medium and a destination medium, such as between two computers communicating over a telecommunications link or network. Each character of the incoming data stream is tested using a finite state machine, which is capable of testing against multiple search strings representing the signatures of multiple known computer viruses. When a virus is detected the incoming data is prevented from remaining on the destination storage medium. Both hardware and software implementations are envisioned, (**See Abstract**).

Hile et al. differs from the claimed invention is that the authentication, encryption, and decryption of an E-mail is not taught in Hile et al.

Kim teaches a system and method for a remote or network-based application service offering virus scanning, sniffing, or detecting of e-mail viruses prior to the e-mail messages arriving at the destination system or server are disclosed. The method protects a computer system that is configured to receive an e-mail message addressed to a destination e-mail address from viruses in an incoming e-mail message, (**See Abstract**), and further teaches that the for an e-mail message which the virus protection software may not be able to scan, such as certain encrypted e-mail messages, the e-mail message may be also be quarantined, (**Column 7, lines 50 - 54**). Kim provides the advantage of authentication, encryption, and decryption of an E-mail.

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Hile by including an authentication, encryption, and decryption of an E-mail as taught by Kim.

One of ordinary skill in the art would have been motivated to make this modification in order provide the advantage of providing the advantage of the authentication, encryption, and decryption of an E-mail.

- **Claims** 23, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hile et al. (US 5,319,776) as applied to claims 1 above, and further in view of Milosvsky et al. (US 6,473,787).

Regarding claims 23, Hile teaches the method according to claim 1, as described above. Hile further teaches a server configured to send outgoing electronic messages on behalf of terminals connected thereto and to deliver incoming electronic messages to the terminals, **[The invention will be described in conjunction with a communications system which may be used to send and receive data via modems over a telecommunications link, (Column 3, lines 7 – 10)];** each terminal being accessed by one or more users, **[In a telecommunications system, often the user of the second computer system 14 will have no direct control over the integrity of files stored on the source medium, (Column 3, lines 45 – 48)];** and, analyzing means to analyze the received traffic log data in accordance with a specified criterion, so as to identity those electronic messages that satisfy the criterion, **[To combat the problem, others have employed virus scanning programs which read the files stored on a storage medium, looking for known virus signatures, (Column 1, lines 32 – 35)].**

Hile et al. differs from the claimed invention is that logging means arranged to generate log data relating to one or more traffic characteristics associated with electronic messages is not taught in Hile et al.

Milosvsky teaches a system for routing electronic mails to one of a plurality of support persons in a processing center is disclosed. Each person has a skill set that is suitable for responding to a certain type of e-mails. The system comprises an e-mail server for receiving the e-mail from a sender, an information extractor for extracting relevant information from the e-mail, and a router for routing the e-mail, **(See Abstract)**, and further teaches that when a support person starts 15 to work, he/she logs in so that stat-server 112 knows who is working in center 100 and how to reach the support person, **(Column 7, lines 50 - 54)**. Milosvsky provides the advantage of logging means arranged to generate log data relating to one or more traffic characteristics associated with electronic messages.

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify Hile by including logging means arranged to generate log data relating to one or more traffic characteristics associated with electronic messages by Milosvsky.

One of ordinary skill in the art would have been motivated to make this modification in order provide the advantage of logging means arranged to generate log data relating to one or more traffic characteristics associated with electronic messages.

Regarding claim 24, Hile teaches a server, the server comprising identifying means arranged to identify the destination of the identified electronic messages, **[Fig.1, step 40]**;

processing means arranged to send a message to each of the identified destinations,

[The invention will be described in conjunction with a communications system which may be used to send and receive data via modems over a telecommunications link, (Column 3, lines 7 – 10)];

requesting suspension of delivery of the identified electronic messages, **[When a virus is detected the incoming data is prevented from remaining on the destination storage medium, (See Abstract)].**

Conclusion

The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See **PEP 707.05(c)**.

The following are analogous art because they are from the same field of endeavor of Server for Sending Electronics Messages:

- Hile et al. (US 5,319,776).
- Sorkin et al. (US 2002/0162017).
- Kim et al. (US 6,701,440).
- Milosvsky et al. (US 6,473,787).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **Shaq Taha** whose telephone number is 571-270-1921.

The examiner can normally be reached on 8:30am-5pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Jeff Pwu** can be reached on 571-272-6798.

Application/Control Number:
10/522,919
Art Unit: 2146

Page 25

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

01/23/07

S. Taha


JEFFREY PWU
SUPERVISORY PATENT EXAMINER